

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

04/10/2012

SUBJECT:

Vulnerability in .NET Framework Could Allow Remote Code Execution (MS12-025)

OVERVIEW:

A vulnerability has been discovered in the Microsoft .NET Framework which could allow an attacker to take complete control of an affected system. Microsoft.NET is a software framework for applications designed to run under Microsoft Windows. The vulnerability can be exploited if a user visits or is redirected to a malicious web page, or runs a specially crafted Microsoft .NET application.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft .NET Framework 1.0 SP3
- Microsoft .NET Framework 1.1 SP1
- Microsoft .NET Framework 2.0 SP2
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4.0

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in the Microsoft .NET Framework that could allow an attacker to take complete control of an affected system. The vulnerability is caused by .NET improperly validating parameters before passing them to a function. This vulnerability can be exploited in any of the following scenarios:

In the first scenario, an attacker could upload malicious ASP.NET code to a web server that hosts user-created content. Successful exploitation could result in the attacker gaining the same privileges as the service account associated with the application pool identity. Depending on the privileges granted to the service account and on the application pool configuration, an attacker might be able to take control of other application pools on the Web server or be able to take complete control of the affected system.

In the second scenario, exploitation could occur if a user visits a specially crafted website that hosts malicious XBAP (Extensible Application Markup Language Browser Application) content.

In the third scenario, an attacker can exploit this issue by creating Windows .NET applications to bypass Code Access Security (CAS) restrictions.

Successful exploitation of the second and third scenarios could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all services.
- Unless there is a business need to do otherwise, consider disabling XAML browser applications (XBAP) in Internet Explorer.

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/bulletin/ms12-025>

Security Focus:

<http://www.securityfocus.com/bid/52921>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0163>